CONFIGURE SIEM SECURITY OPERATIONS USING MICROSOFT SENTINEL (SC-5001)

Course Code: 834034

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace.

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel analytics rules, and responding to threats with automated responses.

What You'll Learn

Students will learn to,

- Create and manage Microsoft Sentinel workspaces
- Connect Microsoft services to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Configure SIEM security operations using Microsoft Sentinel

Who Needs to Attend

Students wishing to configure SIEM security operations using Microsoft Sentinel.

Prerequisites

- Fundamental understanding of Microsoft Azure
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in Microsoft Sentinel

skillsoft global knowledge™

CONFIGURE SIEM SECURITY OPERATIONS USING MICROSOFT SENTINEL (SC-5001)

Course Code: 834034

CLASSROOM LIVE	$675 USD	1 Day

Classroom Live Outline

Module 1: Create and manage Microsoft Sentinel workspaces

- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Manage a Microsoft Sentinel workspace

Module 2: Connect Microsoft services to Microsoft Sentinel

- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Microsoft Sentinel

Module 3: Connect Windows hosts to Microsoft Sentinel

- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

Module 4: Threat detection with Microsoft Sentinel analytics

- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Module 5: Automation in Microsoft Sentinel

- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel

Module 6: Configure SIEM security operations using Microsoft Sentinel

- Create and configure a Microsoft Sentinel workspace

- Deploy Microsoft Sentinel Content Hub solutions and data connectors
- Configure Microsoft Sentinel Data Collection rules, NRT Analytic rule and Automation
- Perform a simulated attack to validate Analytic and Automation rules

skillsoft global knowledge™

CONFIGURE SIEM SECURITY OPERATIONS USING MICROSOFT SENTINEL (SC-5001)

Course Code: 834034

VIRTUAL CLASSROOM LIVE	$675 USD	1 Day

Virtual Classroom Live Outline

Module 1: Create and manage Microsoft Sentinel workspaces

- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Manage a Microsoft Sentinel workspace

Module 2: Connect Microsoft services to Microsoft Sentinel

- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Microsoft Sentinel

Module 3: Connect Windows hosts to Microsoft Sentinel

- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

Module 4: Threat detection with Microsoft Sentinel analytics

- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Module 5: Automation in Microsoft Sentinel

- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel

Module 6: Configure SIEM security operations using Microsoft Sentinel

- Create and configure a Microsoft Sentinel workspace

- Deploy Microsoft Sentinel Content Hub solutions and data connectors
- Configure Microsoft Sentinel Data Collection rules, NRT Analytic rule and Automation
- Perform a simulated attack to validate Analytic and Automation rules

Jun 2 - 2, 2025 | 9:00 AM - 5:00 PM EDT

Aug 25 - 25, 2025 | 9:00 AM - 5:00 PM EDT

Oct 6 - 6, 2025 | 9:00 AM - 5:00 PM EDT

Jan 5 - 5, 2026 | 9:00 AM - 5:00 PM EST

CONFIGURE SIEM SECURITY OPERATIONS USING MICROSOFT SENTINEL (SC-5001)

Course Code: 834034

PRIVATE GROUP TRAINING	1 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 3:07:45 AM